Downloaded from <https://www.velvetjobs.com/job-descriptions/cyber-information-assurance-analyst>

# Example of Cyber Information Assurance Analyst Job Description

Our growing company is searching for experienced candidates for the position of cyber information assurance analyst. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

## Responsibilities for cyber information assurance analyst

* Must be able to use DOD approved scanning tools to include but not limited to, McAfee HBSS, NESSUS (ACAS), SCC SCAP security configuration scanner, STIG Viewer, and nMAP
* Draft system security plans and other artifacts to satisfy certification and accreditation requirements under Risk Management Framework
* Ensuring systems are operated, maintained and disposed of in accordance with applicable federal and local security policies and procedures
* Work with appointed IASO, SCA and other accrediting team members to remediate and mitigate findings
* Assist in the implementation of the required government policy (i.e., JSIG), make recommendations on process tailoring, participate in and document process activities
* Document the results of Certification and Accreditation activities and technical or coordination activity and prepare the System Security
* Plan (SSP) and update the Plan of Actions and Milestones (POA&M)
* Maintain the day-to-day operations of the in-place security solutions while identifying, investigating and resolving security breaches detected by those systems
* Secondary tasks may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines and procedures conducting vulnerability audits and assessments
* The IT Security Analyst is expected to be fully aware of the enterprise’s security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals

## Qualifications for cyber information assurance analyst

* 8 years of experience total in related IT field, , servers, routers, firewalls
* 2 years of experience with COMSEC policies and procedure
* Army approved Computing Environment Certification (CEC)
* Bachelor's degree in Information Technology or a related field and 5 years of related experience required
* Must have a current CompTIA Security + CE with continuing education in progress for the current year
* Bachelor's degree required with 8 years of experience in related IT field, , servers, routers, firewalls